www.pwc.com/security

Eye of the storm

As the global economy stalls and information security threats such as cyber crime and Advanced Persistent Threats cloud the horizon, many see sunshine and clear skies overhead

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Automotive

Key findings from the 2012 Global State of Information Security Survey®

September 2011

pwc

Rapidly intensifying tropical depressions can develop a small, clear, and circular eye. These eyes can range in width from 2 to 200 miles.

But eyes typically exhibit significant fluctuations in intensity and can create headaches for forecasters.[1]

Predictions aside, what matters most is preparation.

[1] National Hurricane Center

The economic thunderheads of 2008 may have passed. But across the global automotive industry, some clouds still linger over revenue, growth, and margin performance. And visibility into when and how the next cyber threat to information will emerge is poor, at best.

Nonetheless, according to PwC's 2012 Global State of Information Security Survey®, the majority of automotive executives are confident in the effectiveness of their information security practices.

They have an effective strategy in place. They consider their organizations proactive in executing it. And funding expectations are running high.

Yet all is not in order. Security event frequency is up. Third-party risks have begun to increase. And respondents are far more concerned about protecting customer data than they were twelve months ago.

Sunshine overhead can be misleading – especially when it coincides with low barometric pressure. If 2008 was just the initial eyewall, there are high winds ahead – and much preparation to complete. And, given the growing strength of the updrafts across many dimensions of cyber crime, the reasons to do so quickly and strategically are mounting.

Agenda

Section 1.	Methodology
Section 2.	Confidence and progress
Section 3.	Signs of vulnerability and exposure
Section 4.	The greatest opportunities for improvement

Section 1

Methodology

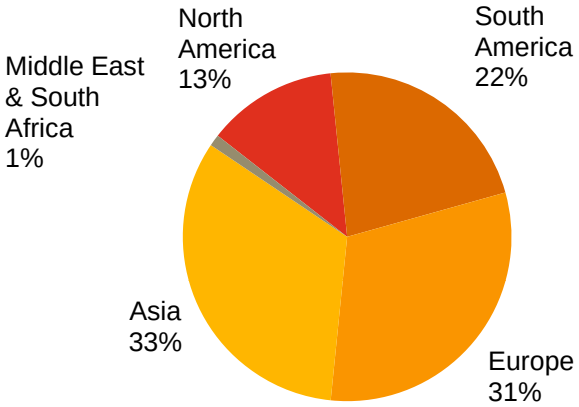
A worldwide study

The 2012 Global State of Information Security Survey®, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 10, 2011 to April 18, 2011.

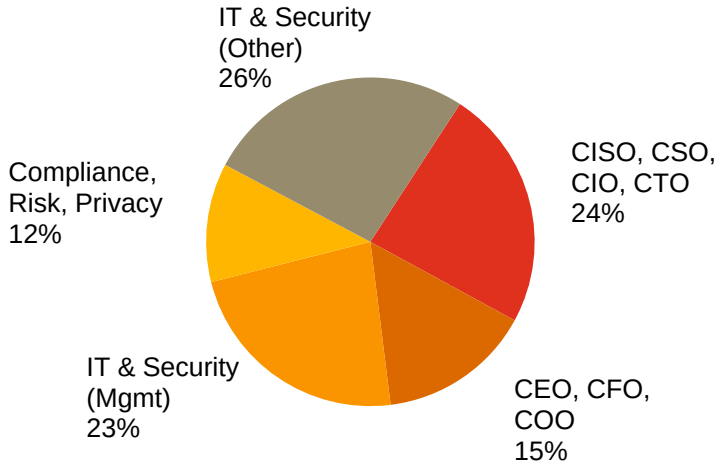
- PwC's 14th year conducting the online survey, 9th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 138 countries
- More than 9,600 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-one percent (31%) of respondents from companies with revenue of $500 million+
- Survey included 265 respondents from the global automotive industry
- The margin of error is less than 1%

Demographics

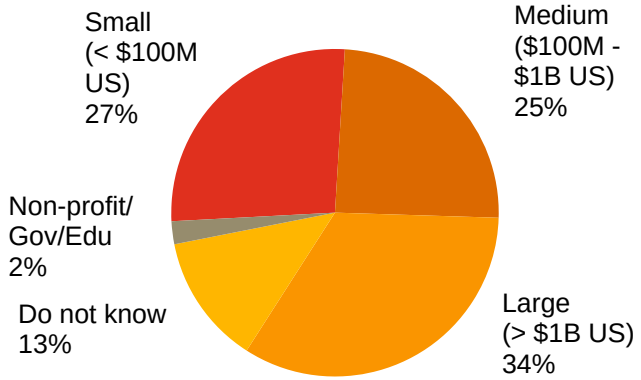
Automotive respondents by region of employment



Automotive respondents by title



Automotive respondents by company revenue size



(Numbers reported may not reconcile exactly with raw data due to rounding)

Section 2

Confidence and progress

Most respondents from the automotive industry see their organization as a "front-runner."

More than half (54%) of this year's automotive industry respondents say their organization has a strategy in place and is proactive in executing it.

Question 26n11: "Which statement best characterizes your organization's approach to protecting information security?"

They are also highly confident in their organization's security.

A clear majority – 83% – of industry respondents are also confident that their organization's information security initiatives are effective.

	2011
Very confident	**38%**
Somewhat confident	**45%**
Total	**83%**

Question 35: "How confident are you that your organization's information security activities are effective?"

Insights into the frequency, type, and source of security breaches have leaped dramatically over the past 12 months.

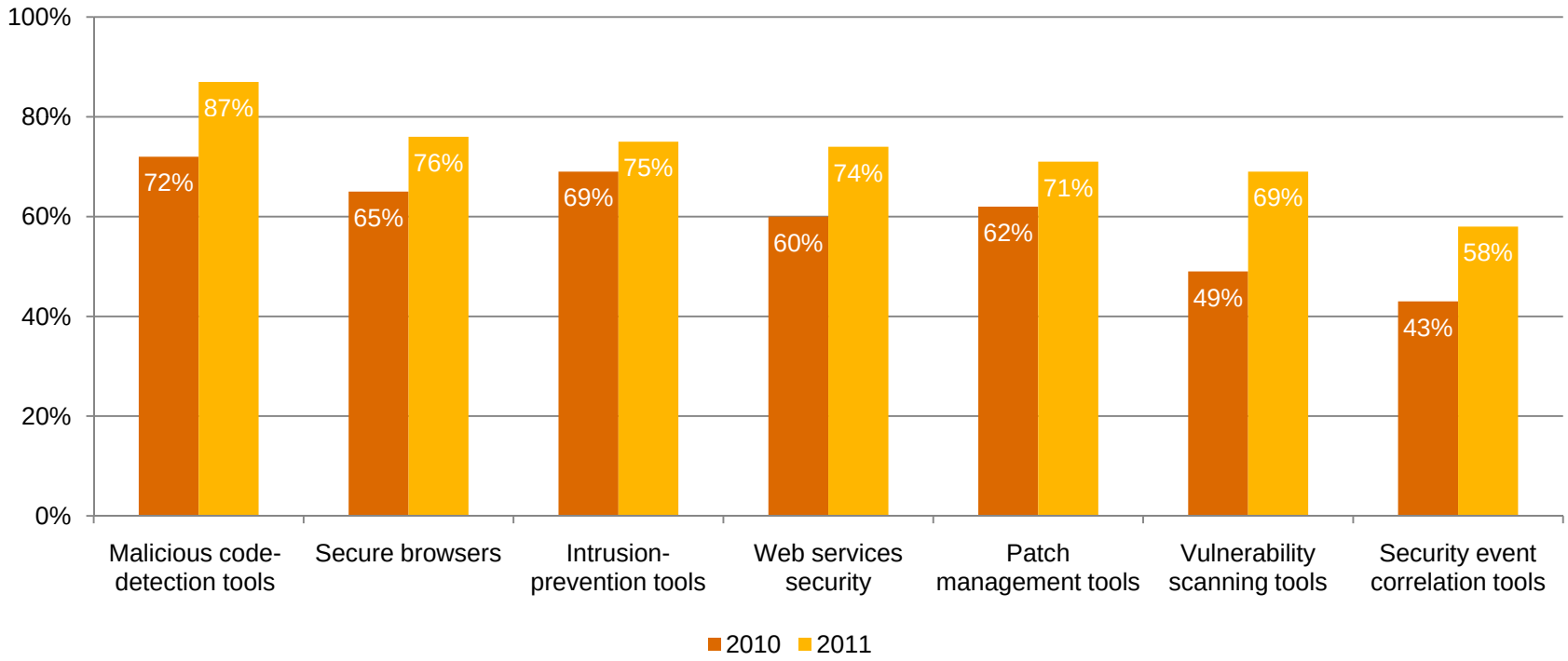
Just a few years ago, as many as 39% of automotive respondents couldn't answer the most basic questions about the nature of security-related breaches. Now, 88% or more of automotive industry respondents can answer specific survey questions about factors such as security event frequency, type, and source.

Respondents who answered "Do not know" or "Unknown"	2007	2008	2009	2010	2011
How many incidents occurred in past 12 months?	39%	33%	24%	16%	**4%**
What type of incident occurred?	34%	47%	36%	25%	**8%**
What was the source of the incident?	N/A	38%	39%	27%	**12%**

Question 19: "Number of security incidents in the past 12 months." Question 20: "What types of security incidents (breach or downtime) occurred?" Question 22: "Estimated likely source of incident." (Totals do not add up to 100%.)

Many automotive companies are proactively adopting safeguards to bolster data security and prevent cyber crime.

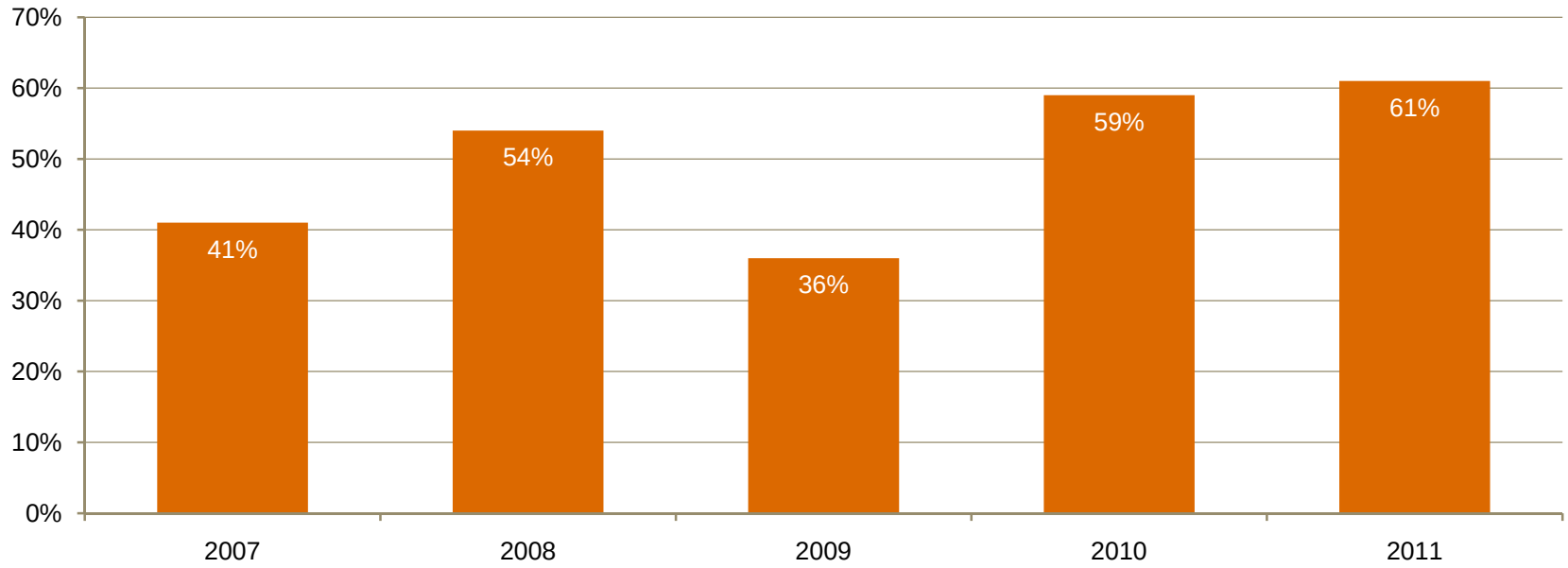
Over the past year, automotive companies have made solid gains in strengthening detection and prevention safeguards to protect information from potential breaches.



Question 18: "What technology information security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

At the same time, most automotive respondents are optimistic about security spending over the next 12 months.

Will security spending in the industry increase? Optimism carries the day. More than half (61%) of automotive industry respondents believe that it will. This level of expectation is the highest it has been in the industry since before the 2008 economic downturn.



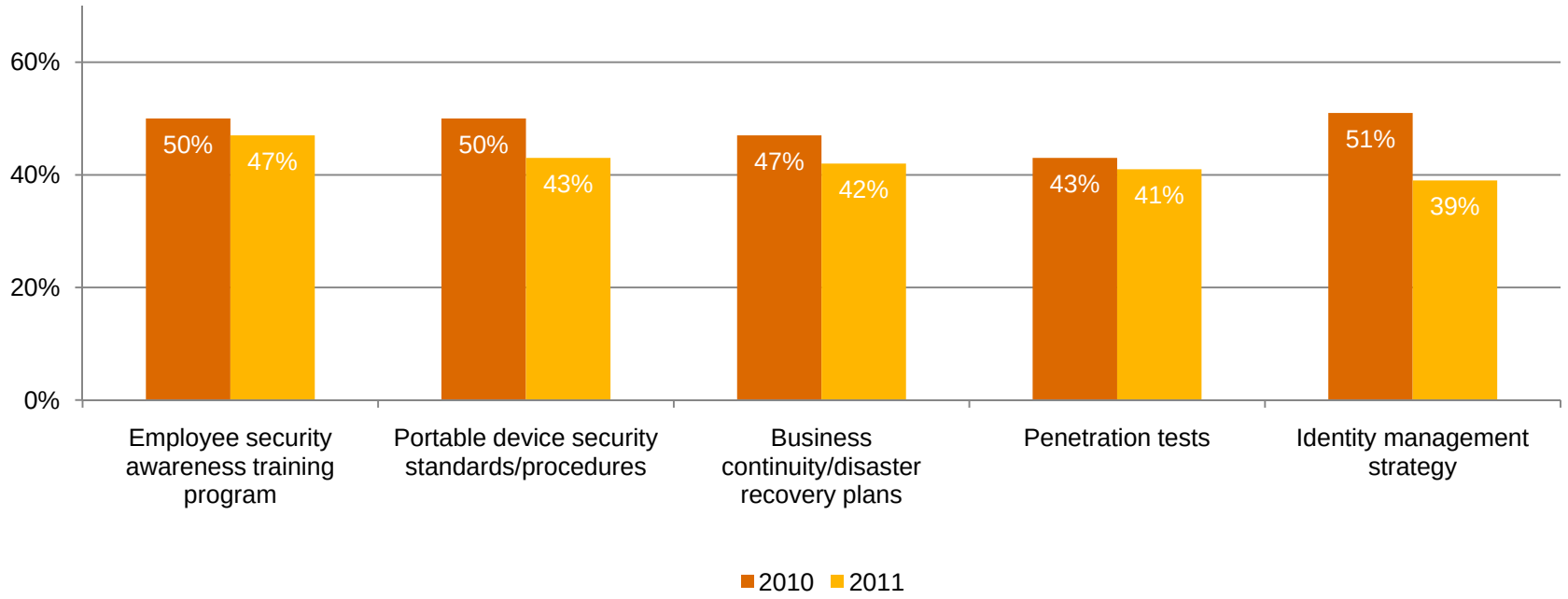
Question 9: “When compared with last year, security spending over the next 12 months will:” (Respondents who answered “Increase up to 10%,” “Increase 11-30%,” or “Increase more than 30%”)

Section 3

Signs of vulnerability and exposure

Advanced Persistent Threats: They can be devastating – but just how prepared are automotive companies to address them?

While 19% of automotive respondents say their organization has a security policy that addresses APT, many lack the tools to combat these new threats.



Question 28" "Which of the following elements, if any, are included in your organization's security policy?" Question 17: "What process information technology security safeguards does your organization currently have in place?" (Not all factors shown. Totals do not add up to 100%.)

Other trends in this year's survey are also troubling. Take the increase in security events, for example.

It is tempting to trumpet the fact that almost one in three (31%) of all automotive industry respondents report no security events in the past year. Yet incidents increased significantly this year among respondents indicating 10 or more negative events.

Number of security incidents	2007	2008	2009	2010	2011
No incidents	16%	26%	17%	27%	31%
1 to 9 incidents	39%	31%	36%	47%	45%
10 to 49 incidents	4%	6%	14%	8%	12%
50 or more incidents	2%	3%	9%	3%	7%

Question 19: "Number of security incidents in the past 12 months." (Totals do not add up to 100%.)

This year's results reveal regression in a key best practice – and a leap in the percentage of CISOs reporting to the CIO.

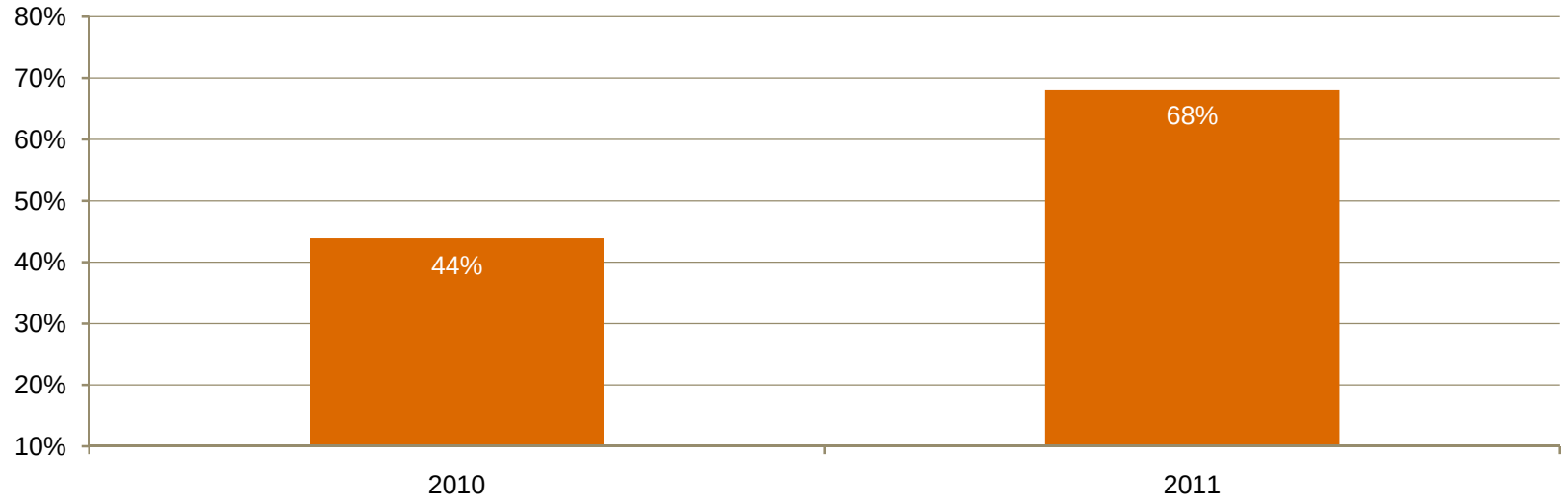
Reversing a multi-year trend, the number of automotive industry respondents who say their Chief Information Security Officer (or equivalent executive) reports to the CIO increased 180% over last year.

Whom the CISO reports to	2007	2008	2009	2010	2011
Board of Directors	24%	28%	24%	33%	**33%**
Chief Executive Officer	35%	28%	41%	44%	**45%**
Chief Financial Officer	6%	6%	11%	19%	**18%**
Chief Information Officer	65%	42%	39%	15%	**42%**

Question 16a: "Where/to whom does your CISO or equivalent senior information security officer report?" (Not all factors shown. Totals do not add up to 100%.)

Concern about protecting customer data has surged this year – though core data protections are often weak or absent.

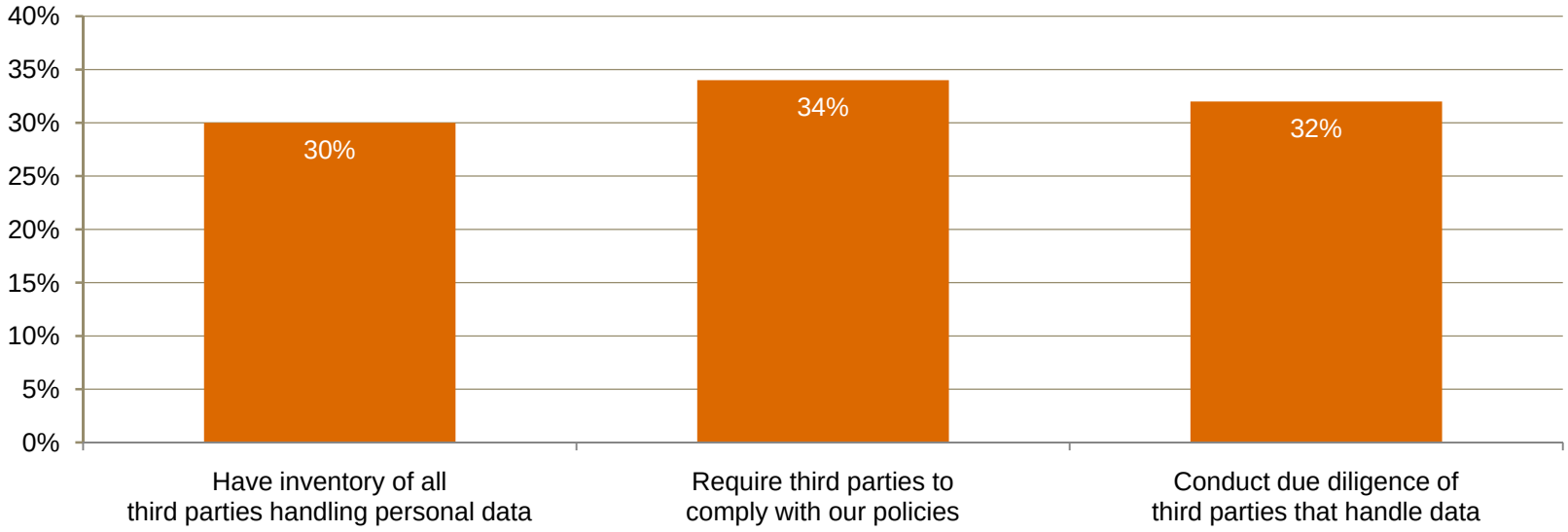
Industry respondents report a tremendous increase (55%) in the level of importance now placed upon protecting customer data – from 44% last year to 68% this year. Yet fewer than half report that their organization keeps an accurate inventory of employee and customer data (40%), has a security policy that addresses data protection, disclosure and destruction (42%) and encrypts backup media (49%).



Question 32n11: "What level of importance does your company place on protecting the following types of information? Customer information" Questions15 and 18 "Which data privacy/technology information security safeguards does your organization have in place?" Question 28: "Which of the following elements, if any, are included in your organization's security policy?"

Third party risk is on the rise.

Since 2008, the percentage of industry respondents that consider partners or suppliers the likely source of security breaches has more than doubled – from 8% to 19%. Is the industry combating this risk? Not necessarily. Many have not yet established strategies and practices governing service providers and other third parties.



Question 22: “Estimated likely source of incident.” Question 15: “Which data privacy safeguards does your organization have in place?” (Not all factors shown. Total does not add up to 100%.)

Section 4

The greatest opportunities for improvement

What's holding security back?

Given the austere spending environment, it would make sense if industry respondents considered insufficient capital one of the leading obstacles to the effectiveness of their organization's information security function.

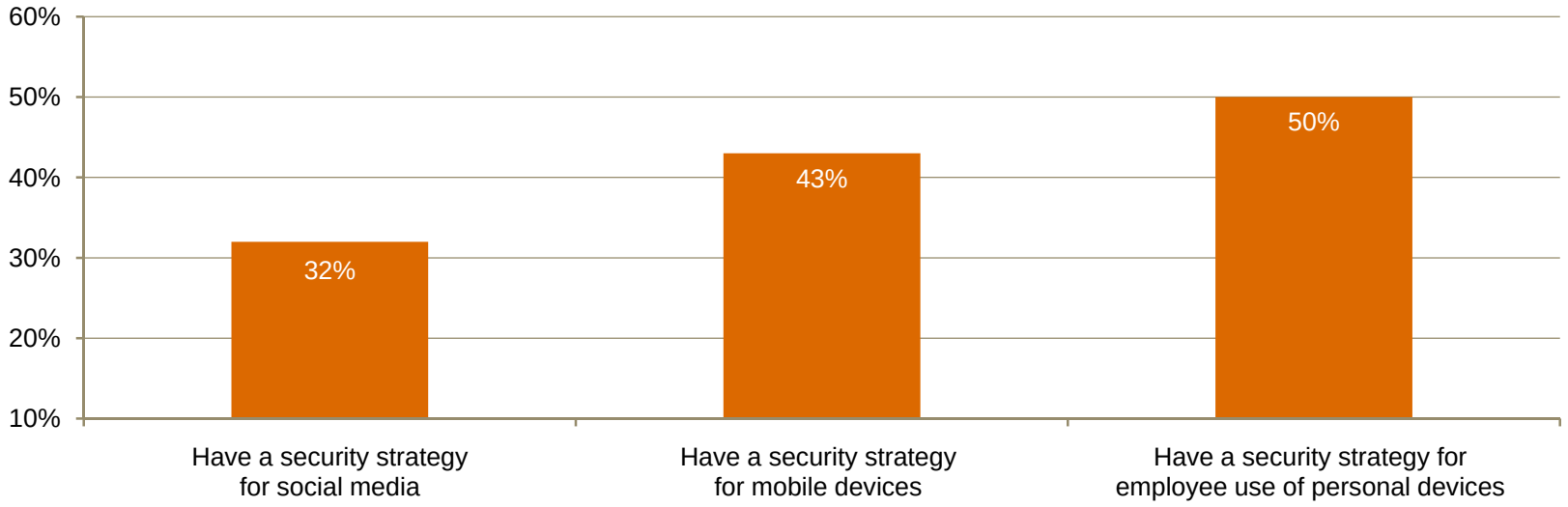
Surprisingly, they don't. More than one out of three point to the lack of an actionable vision, and almost as many reference the absence of an effective information security strategy.

	2011
1. Lack of an actionable vision or understanding	34%
2. Lack of an effective information security strategy	28%
3. Leadership – CEO, President, Board, or equivalent	27%
4. Leadership – CIO or equivalent	27%
5. Insufficient capital expenditures	26%
6. Absence or shortage of in-house technical expertise	23%
7. Insufficient operating expenditures	21%

Question 27n11: "What are the greatest obstacles to improving the overall strategic effectiveness of your organization's information security function?" (Not all factors shown. Total does not add up to 100%.)

Mobile devices and social media: New rules are in effect this year – but adoption has yet to reach critical mass.

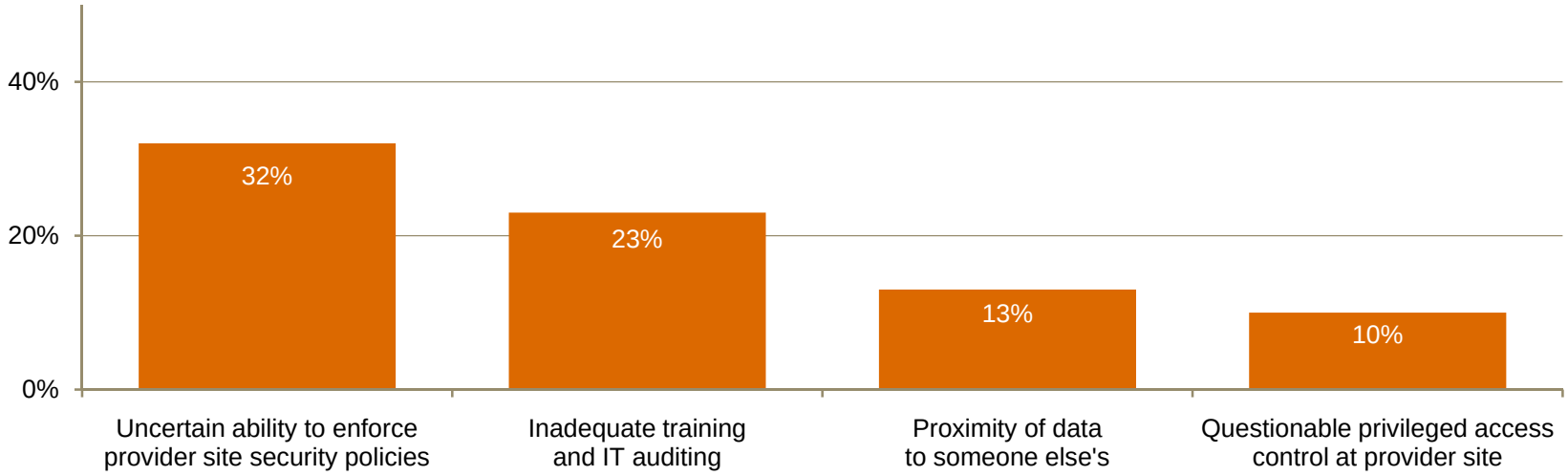
Automotive companies are implementing strategies to keep pace with employee adoption of new technologies – including use of mobile devices and social-networking tools – and are creating rules about how employees can use personal technology within the enterprise.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Cloud computing continues to evolve this year, but many respondents want better enforcement of provider security policies.

This year, almost half (49%) of automotive respondents report that their organization uses cloud services. Among those that have adopted cloud solutions, 77% say the technology has improved their security posture. Responses also revealed that while enforcing provider security policies is seen as the principal security challenge, respondents are also concerned about training as well as multi-tenancy issues.



Question 41: “Does your organization currently use cloud services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS)?” Question 41c: “What impact has cloud computing had on your company’s information security?” Question 41b: “What is the greatest security risk to your cloud computing strategy?” (Not all factors shown. Total does not add up to 100%.)

For more information, please contact:

National Security Contacts

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

Automotive Contacts (North America)

Brian Decker
US Automotive Advisory Leader
313.394.6263
brian.d.decker@us.pwc.com

Michael Compton
Principal
313.394.3535
michael.d.compton@us.pwc.com

Or visit www.pwc.com/giss2012